Speech presented by Adam Graycar, Director,
Australian Institute of Criminology:

"Identity-related fraud"

in Canberra, November 2001

Adam Graycar
November, 2001
Canberra

Some years ago I was a Visiting Professor at UC Berkeley. I had a problem living and working in California, because so many transactions required me to have 2 pieces of photo ID - cashing a cheque, getting a library card, opening a bank account or getting a social security number so I could be paid. I only had one piece of photo ID - my passport, and nobody could believe that coming from a first world country like Australia I did not have 2 pieces of photo ID. After a bit of irregularity I got a university staff card with a photo on it. These pieces of ID didn't prove a great deal - they confirmed, after a fashion, that the person in the photo was the person holding the document (if anyone actually took the trouble to look). They did not, in fact, confirm that the person in the photo who was holding the document was the person I was purporting to be.

As the father of teenagers, there are many things one hears that one doesn't want to know. I'm sure you have you heard the one about the 17 year old borrowing his 19 year old brother's drivers licence to show, if he has to, at the pub. Or the occasional stories about having somebody else sit your university exam for you. Though that may be a bit obsolete now, with so much distance education, and assignments and exams being done on-line, one wonders how the lecturer knows who's writing the assignments?

Even today, all these years after California, I have only 3 pieces of photo ID - my passport, my drivers licence and my pass to get me into Parliament House. How many pieces of photo ID do you have? How many do you need? And do you still look the same as when the photo was first taken?

Of course, when I wanted to cash a cheque in California I had only good and pure intentions in mind. When a 17 year old wants a beer, some may say that on the scale of seriousness, that's pretty low, however, when we get into criminal activities it's pretty serious.

There is a common thread running through almost all crime and that is the desire of offenders to escape detection, arrest, and punishment for their wrongful activities (the exception to this might be certain politically-

motivated crimes in which publicity given to the criminal might be part of what is sought to be achieved).

The techniques used to avoid detection have been diverse throughout history:

- Bushrangers and outlaws invariably used masks to cover their faces and, of course, the armour worn by the members of the Kelly Gang not only had the effect of protecting them from most bullets, but also of disguising their identities.

- Pirates on the high seas sometimes flew the flag of another innocent ship in order to approach their victim without alerting them to their true identity and purpose.

- Murderers have used aliases and planted false evidence in order to commit crimes and incriminate innocent people, sometimes leading to wrongful arrest of those whom they have incriminated, and tragically, sometimes resulting in their execution.

More recently we have seen an escalation in such acts of deception.

- In Canberra, on 25 September 2001, a financial consultant formerly contracted to the Department of Finance and Administration was convicted of defrauding the Commonwealth by transferring $8,735,692 electronically to private companies in which he held an interest. He did this by logging on to the Department's computer network using another person's name and password. He was also able to obscure an audit trial through the use of other employees' logon codes and passwords. He was sentenced in the ACT Supreme Court to 7 years and six months' imprisonment with a non-parole period of 3 years and six months (R v *Muir*, ACT Supreme Court, 25 September 2001).

- In Australia, the Department of Immigration and Multicultural Affairs has been required to investigate cases in which people who have been granted refugee status are not, in fact, who they claim to be. Some have claimed to be from Afghanistan when in fact they have come from Pakistan and may have no legitimate claim to refugee status.

- The alleged terrorists who destroyed the World Trade Centre were said to have used other people's names when undertaking their pilot training and when boarding the aircraft prior to 11 September 2001.

I could spend the rest of the morning giving you examples, though not all identity creation is fraudulent. Actors and performers often use 'stage names' — such as Elton John and Marilyn Monroe.

It all depends on what services and access you want, what you need to demonstrate to get where you want to be, and what those who welcome you as a customer want to satisfy themselves that you are who you say you are. It all comes down to establishing trust.

To arrive in the country or to leave, to get a benefit, or open a bank account you need to establish identity. We have a population of 19 million and the Attorney General's Dept has developed a diagram which shows a flow of 16 million people who each year arrive or depart, get born or die - 16 million pieces of identity that have to be generated each year!

Of people already here, last year the Australian Electoral Commission processed 2.46 million enrolment forms (and it wasn't even an election year); ATO issues half a million tax file numbers, Centrelink processed 4.4 new claims or re-grants; DFAT issued 1.4 million passports. And this is a drop in the ocean when we start to think of all the Commonwealth and State agencies, not to mention private sector companies, banks, credit card companies, investment houses, schools and universities, professional associations, professional regulatory authorities etc etc etc.

For those of us here today there are several types of issues we need to be aware of.

- Awareness of the types of identity fraud, the variations, the costs and the implications

- Awareness of means of assessing the risks posed to your organisations

- Awareness of co-operative mechanisms with other agencies which have similar problems or which hold data that you may need to match

Awareness of these issues needs to be raised at various organisational levels within agencies:

- Tools and procedures for front line staff
- Awareness for middle level managers
- Broad policy issues for senior staff

Quantifying the Scale of the Problem

As senior managers you probably have some idea of the dollar value of the losses to your agencies do to identity fraud. One of the key facts that we need to know in assessing the scale of the problem of identity-related fraud is how much money is being lost to this type of criminal activity.

Knowing how much has been lost in cases involving fraud has important implications for deciding whether or not to embark on a prosecution, and also for justifying, in terms of Return on Investment, any expenditure associated with taking legal action.

Knowing exactly how much has been lost to an organisation following fraud is also important for the costing of future fraud prevention initiatives.

Sometimes organisations may be unaware of how much they have lost in individual cases and it will only be after the case has been investigated by forensic accountants and the police that the full extent of losses will become apparent.

Bearing these considerations in mind, attempts have been made to quantify how much is lost to identity-related fraud in Australia. An Inter-agency Working Group on the cost of identity-related fraud chaired by AUSTRAC is currently examining this question of quantification.

At the AIC we have estimated that the cost of crime is up to 4% of Gross Domestic Product (GDP). In 1999-2000, Australian GDP was $632 billion. Approximately 28% of the cost of all crime relates to fraud and dishonesty.

Research currently being carried out by the AIC in conjunction with PricewaterhouseCoopers, puts the percentage of large-scale identity-related

fraud cases dealt with by police in Australia in 1998-99 out of the total number of all serious fraud cases dealt with at around 41%.

It is possible, therefore to calculate a very rough estimate of the cost of identity-related fraud as being around $2.9 billion a year. This could be a bit rubbery. [$632 billion (GDP) x 0.04 (crime costs) x 0.28 (fraud) x 0.41 (ID fraud) = $2.9 billion]

Clearly this is a very rough estimate, and is probably an under-estimate, but is in line with some other indications of the extent of the problem.

- Recently, the New South Wales Registrar of Births, Deaths and Marriages carried out a trial verifying birth certificates used to open bank accounts with Westpac. It was found that 13% of birth certificates presented were not an exact match with the records held by the issuing authority.

- In 1999, Centrelink detected about $12 million worth of fraud involving false identity.

- About one quarter of reported frauds to the AFP involve the assumption of false identities.

In the United States in 2000, businesses and consumers were said to have lost US$35 billion to identity thieves. Credit card fraud makes up 50% of identity theft complaints to the Federal Trade Commission. Identity theft complaints to the Federal Trade Commission (FTC) rose from 400 per week in March 2000 to 1,700 per week in December 2000 accounting for 23% of the 80,000 fraud complaints received by the agency
It is of interest to note that ID theft victims either knew or were related to the criminals in 14% of cases reported.

And in April this year in Tijuana, Mexico, two armed robbers ambushed a delivery van in order to steal 6,000 identity cards that were being delivered to consulates in Mexico. The cards would allow entry into the United States and are estimated to be worth more than US$1 million on the black market.

TYPES OF FALSE IDENTITY

Some people steal somebody else's identity, and others create false identities.

Identities can be stolen or created using legitimate or forged documents.

Legitimate documents might be stolen from a living or deceased person, while legitimate documents might involve changed names or variations of real names.

Names are interesting - people change their names for all sorts of reasons, use maiden names or married names, use their mother's maiden name instead of their father's name, and do all of the above inconsistently. One of my daughters uses my name, the other her mother's, my wife uses her maiden name, and her sister her mother's maiden name - and we are a simple family not in the business of defrauding anyone! With an increasing non-European immigrant community we find ourselves with decisions about the order of Asian names, or the proliferation of names like Chan, Ngyuen, Mohammed, Abdul etc. This is not to mention the fact that in the Melbourne telephone directory there are approximately 8,000 Smiths (including a number of Russell Smiths - one of whom is here today), and almost 4,000 Nguyens.

Forged documents can be created to support a fictitious identity - a fictitious name, date of birth etc can be forged onto documents, or misappropriated real name, personal details and registration details forged onto documents. The technologies that allow us to do wonderful desktop publishing allow villains to create illegal documents that look convincingly real.

And, of course, there are many cases where people appear who have no documents at all, and about whom judgements must be made.

PREVENTION AND COUNTER MEASURES

It is often said that crime follows opportunity. Whenever there is an opportunity to get some money, obtain a benefit, or have access to something highly desirable, there are opportunities for illegality, and in these areas there is always the need for people to have documents and information that can be used to prove their identity with certainty.

To make crime harder to commit there are three general situational strategies that we might ponder in looking at identity fraud,

- Increasing the effort
- Increasing the risk
- Reducing the rewards

I want you to think about whether these strategies are available to you, and how you make sure your staff can respond.

Increasing the effort can be both technological and operational. At one stage anyone could open a bank account by walking into a bank with $2 in their hand. Now the *Financial Transaction Reports Regulations* require that sufficient evidence be produced at the time a bank account is opened to ensure that the customer may be located should any default later occur. There are also substantial penalties which apply where accounts are opened in a name other than that which the person usually uses.

The so-called 100-point system requires that evidence be produced in the form of primary documents (such as a birth certificate, current passport, or certificate of citizenship—each of which carries seventy points), and secondary documents (such as a driver's licence, public employee or student identification card—each worth forty points; or a credit card, Medicare card, or council rates notice—each worth twenty-five points). A variety of other documents may be used to verify one's name and address, each carrying differing numbers of points.

Both primary and secondary documents were not created, however, with the intention that they be used for identification purposes. As a result, they often do not have adequate security features in place which makes them susceptible to counterfeiting and alteration.

One means of increasing the effort was to require the 100 points. There may be similar opportunities in your agencies for increasing the effort.

Another means of increasing the effort is for documents or cards to be created which can be used to identify people with certainty, and which are designed specifically so as to make them difficult to counterfeit or alter. Such identifiers could then be used to establish identity for all commercial and private transactions or business relationships where it is essential to

identify the participants accurately, such as when opening bank accounts or registering for government benefits. As electronic commerce becomes more widely used, the need to identify people to whom encrypted key tokens will be issued, will also become of critical importance.

What is also important from a policy perspective is the need for agencies to be able to verify the legitimacy of documents presented for proof of identity purposes with the issuing agency. For example, an officer of the Health Insurance Commission needs to know that a New South Wales driver's licence tendered by someone wishing to obtain a Medicare card was in fact issued by the NSW Roads and Traffic Authority to the person in question.

Technologically the effort can be increased by a range of passwords, PINs, and unique identifiers for people to gain access to that which they should be able to gain access. Technology is moving quickly on that front. There are down sides, as well - I often can't get into websites because I simply can't remember which of my many log on names or PINs goes with that account.

There are also biometric identifiers (such as fingerprints or retinal images) which are being used when individuals first make contact with organisations and are now being used by a range of public and private sector organisations including hospitals, banks, and retail stores. However, there only confirm that the person is the person who first made the contact (and who may have stolen or assumed another identity!)

Increasing the risk involves your agencies setting in place procedures for detecting people who do the wrong thing, and I won't spend any time on that now. The only point I want to make here is that there are significant data matching opportunities, but at the same time significant privacy considerations - and this is going to be a lulu of a debate!!

Reducing the rewards involves a range of legislative responses and organisational activities. Russell Smith has documented these in some detail including the use of increased penalties and the confiscation of assets.

I did not think that an occasion like this was the right time to do a long and ponderous analysis of all the issues. These will be unfolded over time.

The steps which can be taken to prevent identity-related fraud depend upon a range of considerations. These are:

- the likelihood that the risk will be realised;
- the cost of the countermeasures;
- the effectiveness of the technologies used;
- the user-friendliness of systems;
- privacy concerns if data-matching is contemplated; and
- possible negative consequences on the behaviour of users.

It might be possible to prevent all forms of identity-related fraud but the solutions may simply be too costly, unwieldy, and authoritarian to be acceptable.

In certain high-risk areas, however, greater precautions need to be taken to check the validity of documents relied on or other more secure forms of personal identification need to be used.

Technology will provide some of the solutions but these need to be supported by a simple and effective legal regime to ensure that instances of abuse can be prosecuted and that individual privacy is safeguarded.

What is of critical importance, however, is for people to be made aware of the risks of identity-related fraud and how to protect themselves.

Taking action after a crime has been committed is difficult, costly and often impractical. Commercial and personal reputations are often hard to repair and offenders often impossible to find.

What I wanted to do today was to introduce you to the concept of identity-related fraud and to let you know about some of the work we at the AIC are doing on it. Russell Smith and his team have been examining the area, they have published on the issues and ramifications, and preventive and counteractive mechanisms. The AIC's training unit is turning a lot of their material into training materials focussing on awareness of identity-related fraud and risk assessment.

By your being here, you know that keeping up-to-date on the new risks of identity-related fraud is essential for senior executives, as new vulnerabilities are created all the time, and previous crime prevention solutions are overcome by more knowledgeable offenders.

The Way Forward

To conclude, I would like to leave you with three observations on how we should respond to identity-related fraud in the future.

• *The first concerns awareness-raising of the nature and extent of the risks involved.*

There is now considerable information available about the nature of these risks and how to avoid them. People need to be taught how to protect themselves and how to avoid situations of high risk. Managers need to make sure that their staff are adequately trained in detecting possible acts of deception and in dealing with them effectively. And, of course, effective risk assessment procedures need to be in place.

• *The second involves making effective use of existing strategies.*

Many of the solutions to identity-related fraud already exist. People, however, have neglected to make full use of them in order to simplify their business and personal lives. Sometimes we are too busy to change computer access passwords or to pick up the phone to check with a referee about a new employee. Our staff might think it unnecessary to call an issuing authority to confirm the validity of a document that someone has produced.

• *Finally, there is the need to develop and use new technologies.*

New technological solutions such as public key systems, biometrics and data-matching are being developed all the time. Although the cost of some may be large, resources need to be given to such R&D and, most importantly, any new solutions should be properly evaluated in order to test their effectiveness. Assessments also need to be made of the potential social and privacy implications which the use of some new technologies entails. The importance of these concerns should not be under-estimated.

As in all areas of fraud control, keeping one step ahead of criminals is an on-going task that requires time, commitment, and resources. We are not an operational agency, but we work closely and harmoniously with those

agencies that are, and we are always happy to look at blending our knowledge and skills with yours, and the first steps here are a set of training courses for middle managers and supervisors, details of which are in your folders.